

PROCEDURE 5. ELECTRONIC SURVEILLANCE

PART 1: ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSESA. APPLICABILITY

This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and applies to electronic surveillance, as defined in that Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act.

B. GENERAL RULES

1. Electronic surveillance pursuant to the Foreign Intelligence Surveillance Act. A DoD intelligence component may conduct electronic surveillance within the United States for foreign intelligence and counterintelligence purposes only pursuant to an order issued by a judge of the court appointed pursuant to the Foreign Intelligence Surveillance Act of 1978 (reference (b)), or pursuant to a certification of the Attorney General issued under the authority of section 102(a) of the Act.

2. Authority to request electronic surveillance. Authority to approve the submission of applications or requests for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (reference (b)) shall be limited to the Secretary of Defense, the Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, and the Director of the National Security Agency. Applications for court orders will be made through the Attorney General after prior clearance by the General Counsel, DoD. Requests for Attorney General certification shall be made only after prior clearance by the General Counsel, DoD.

3. Electronic surveillance in emergency situations.

a. A DoD intelligence component may conduct electronic surveillance within the United States in emergency situations under an approval from the Attorney General in accordance with section 105(e) of reference (b).

b. The head of **any** DoD intelligence component may request that the DoD General Counsel seek such authority directly from the Attorney General in an emergency, if it is not feasible to submit such request through an official designated in subsection B.2., above, provided the appropriate **official** concerned shall be advised of such requests as soon as possible thereafter.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 2: ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES

A. APPLICABILITY

This part of Procedure 5 applies to electronic surveillance, as defined in Appendix A, for foreign intelligence and counterintelligence purposes directed against United States persons who are outside the United States, and who, **under** the circumstances, have a reasonable expectation of privacy. It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part 1 and the regulation of "signals intelligence activities" under Part 3, so that the intentional interception for **foreign intelligence and** counterintelligence purposes of all wire or radio communications of persons within the United States and against United States persons abroad where such persons enjoy a reasonable expectation of privacy is covered by one of the three parts. In addition, this part governs the use **of** electronic, mechanical, or **other** surveillance devices for foreign intelligence and counterintelligence purposes against a United States person abroad in circumstances where such person has a reasonable expectation of privacy. This part does not apply to the electronic surveillance of communications of other than United States **persons** abroad or the interception of the communications of United States persons abroad that do not constitute electronic surveillance.

B. EXPLANATION OF UNDEFINED TERMS

1. Electronic surveillance is "directed against a United States person" when the surveillance is intentionally targeted against or designed to intercept the communications of that person. Electronic surveillance directed against persons who are not United States persons that results in the incidental acquisition of **the communications** of a United States person does not thereby become electronic surveillance directed against a United States person.

2. Electronic surveillance is "outside the United States" if the person against whom the electronic **surveillance** is directed is physically outside the United States, regardless of the location at which surveillance is conducted. For example, the interception of communications that originate and terminate outside the United States can be conducted from within the **United States** and still fall under this part rather than Part 1.

c. PROCEDURES

Except as provided in section D., below, DoD intelligence components may conduct electronic surveillance **against a United States** person who is outside the United States for foreign intelligence and counterintelligence purposes only if the surveillance is approved by the Attorney General. Requests for approval will be forwarded to the **Attorney General by an** official designated in section E1., below. Each request shall include:

1. An identification or description of the target.

2. A statement of the facts supporting a finding that:

a. There is probable cause to believe the target of the electronic surveillance is one of the following:

(1) A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;

(2) A person who is an officer or employee of a foreign power;

(3) A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

(4) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

(5) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to **information** or material classified by the United States to which such person has access.

b. The electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence.

c. The significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance could not reasonably be obtained by other less intrusive collection techniques.

3. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance.

4. A description of the means by which the electronic surveillance will be effected.

5. If physical trespass is required to effect the surveillance, a statement of facts supporting a finding that the means involve the least amount of intrusion that will accomplish the objective.

6. A statement of period of time, not to exceed 90 days, for which the electronic surveillance is required.

7. A description of the expected dissemination of the product of the surveillance, including a description of the procedures that will govern the retention and dissemination of communications of or concerning United States persons other than those targetted, acquired incidental to such surveillance.

D. ELECTRONIC SURVEILLANCE IN EMERGENCY SITUATIONS

Notwithstanding section C. , above, a DoD intelligence component may conduct surveillance directed at a United States person who is outside the United States in emergency situations under the following limitations:

1. Officials designated in section E., below, may authorize electronic surveillance directed at a United States person outside the United States in emergency situations, when securing the prior approval of the Attorney General is not practical because:

a. The time required would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to the national security;

b. A person's life or physical safety is reasonably believed to be in immediate danger; or

c. The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

2. Except for actions taken under paragraph D.1.b., above, any official authorizing such emergency surveillance shall find that one of the criteria contained in paragraph C.2.a., above, is met. Such officials shall notify the DoD General Counsel promptly of any such surveillance, the reason for authorizing such surveillance on an emergency basis, and the expected results.

3. The Attorney General **shall** be notified by the General Counsel, DoD, as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and such other information as may be required to authorize continuation of such surveillance.

4. Electronic surveillance authorized pursuant to this section may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours.

E. OFFICIALS AUTHORIZED TO REQUEST AND APPROVE ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES

1. The following officials may request approval of electronic surveillance outside the United States under section C., above, and approve emergency surveillance under section D., above:

a. The Secretary and Deputy Secretary of Defense.

b. The Secretaries and Under Secretaries of the Military Departments.

c. The Director and Deputy Director of the National Security Agency/Chief, Central Security Service.

2. Authorization for emergency electronic surveillance under section D. may also be granted by:

a. Any general or flag officer at the overseas location **in** question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered; or

b. The Deputy Director for Operations, National Security Agency.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 3: SIGNALS INTELLIGENCE ACTIVITIESA. APPLICABILITY AND SCOPE

1. This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection, retention, and dissemination of foreign communications and military tactical communications. Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto.

2. This part of Procedure 5 shall be supplemented by a classified Annex promulgated by the Director, National Security Agency/Chief, Central Security Service, which shall also be approved by the Attorney General. That regulation shall provide that signals intelligence activities which constitute electronic surveillance, as defined in Parts 1 and 2 of this procedure, will be authorized in accordance with those parts. Any information collected incidentally about United States persons **shall** be subjected to minimization procedures approved by the Attorney General.

B. EXPLANATION OF UNDEFINED TERMS

1. Communications concerning a United States person are those in which the United States **person** is identified in the communication. A United States person is **identified** when the person's name, unique title, address or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A reference to a product by brand name or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Monroe Doctrine," is not an identification of a United States person.

2. Interception means the acquisition by the United States Signals Intelligence system through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signals.

3. Military tactical communications means United States and allied military exercise communications within the United States and abroad necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

4. United States person. For purposes of signals intelligence activities only, the following guidelines will **apply** in determining whether a person is a United States person:

a. A person known to be currently in the United States will be treated as a United States person **unless** the nature of the person's communications or other available information concerning the person gives rise to a reasonable belief that such person is not a United States citizen or permanent resident alien.

b. A person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.

c. A person known to be an alien admitted for permanent residence may be assumed to have lost status as a United States person if the person leaves the United States and it is known that the person is not in compliance with the administrative formalities provided by law that enable such persons to reenter the United States without regard to the provisions of law that would otherwise restrict an alien's entry into the United States. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

d. An unincorporated association whose headquarters are located outside the United States may be presumed not to be a United States person unless the collecting agency has information indicating that a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence.

5. United States Signals Intelligence System means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the military services authorized to conduct signals intelligence and such other entities (other than the Federal Bureau of Investigation) as are authorized by the National Security Council or the Secretary of Defense to conduct signals intelligence. FBI activities are governed by procedures promulgated by the Attorney General.

c. PROCEDURES

1. Foreign communications. The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this procedure.

2. Military tactical communications. The United States Signals Intelligence System may collect, process, retain, and disseminate military tactical communications that are also communications of or concerning United States persons but only in accordance with the classified annex to this procedure.

a. Collection. Collection efforts will be conducted in the same manner as in the case of signals intelligence for foreign intelligence purposes and must be designed in such a manner as to avoid to the extent feasible the intercept of communications not related to military exercises.

b. Retention and processing. Military tactical communications may be retained and processed without deletion of references to United States persons who are **participants** in, or are otherwise mentioned in exercise-related communications, provided that the communications of United States persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible.

c. Dissemination. Dissemination of military tactical communications and exercise reports or information files derived from such communications shall be limited to those authorities and persons participating **in or** conducting reviews **and** critiques of such exercise.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 4: TECHNICAL SURVEILLANCE COUNTERMEASURESA. APPLICABILITY AND SCOPE

This part of Procedure 5 applies to the use of electronic equipment to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance. It implements section 105(f)(2) of the Foreign Intelligence Surveillance Act (reference (b)).

B. EXPLANATION OF UNDEFINED TERMS

The term technical surveillance countermeasures refers to activities authorized pursuant to DoD Directive 5200.29 (reference (c)), and, as used in this procedure, refers to the use of electronic surveillance equipment, or electronic or mechanical devices, solely for determining the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, or for determining the susceptibility of electronic equipment to unlawful electronic surveillance.

C. PROCEDURES

A DoD intelligence component may use technical surveillance countermeasures that involve the incidental acquisition of the nonpublic communications of United States persons without their consent, provided:

1. The use of such countermeasures has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken;

2. The use ~~of~~ such countermeasures is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

3. Access to the content of communications acquired during the use of countermeasures is limited to persons involved directly in conducting such measures, and any content acquired is destroyed as soon as practical or upon completion of the particular use. However, if the content is acquired within the United States, only information which is necessary to protect against unauthorized electronic surveillance, or to enforce Chapter 119 of title 18, United States Code (reference (d)) and Section 605 of the Communication Act of 1934 (reference (e)), may be retained and disseminated only for these purposes. If acquired outside the United States, information which indicates a violation of federal law, including the Uniform Code of Military Justice (reference (f)), or a clear and imminent threat to life or property, may also be disseminated to appropriate law enforcement authorities. A record of the types of communications and information subject to acquisition by the illegal electronic surveillance equipment may be retained.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 5: DEVELOPING , TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENTA. APPLICABILITY

This part of Procedure 5 applies to developing, testing, or calibrating electronic equipment that can intercept or process communications and **non-**communications signals. It also includes research and development that needs electronic communications as a **signal** source.

B. PROCEDURES1. Signals authorized for use.

a. The following may be used without restriction:

- (1) Laboratory-generated signals.
- (2) Communications signals with the consent of the communicator.
- (3) Communications in the commercial or public **service** broadcast bands.

(4) **Communications transmitted** between terminals located outside of the United States not used by any known United States person.

(5) **Noncommunications** signals (including telemetry, and radar).

b. Communications subject to lawful electronic surveillance under the provisions of Parts 1, 2, or 3 of this procedure may be used subject to the minimization procedures-applicable to such surveillance.

c. Any of the following may be used subject to the restrictions of subsection **B.2.**, below.

(1) Communications over official government communications circuits with consent from an appropriate official of the controlling agency.

(2) Communications in the citizens and amateur-radio bands.

d. Other signals may be used only when it is determined that it is not practical to use the signals described above and it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. The restrictions of subsection **B.2.**, below, **will apply in** such cases. The Attorney General must approve use of signals pursuant to this subsection for the purpose of development, testing, or calibration when the period of use exceeds 90 days. When Attorney General approval is required, the DoD intelligence component shall submit a test proposal to the General Counsel, DoD, or the NSA General Counsel for transmission to the Attorney General **for approval**. The test **proposal** shall state the requirement for a period beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of **any signals** or communications **acquired during** the activity.

2. Restrictions.

For signals described in paragraph **B.1.c.** and d., above, the following restrictions apply:

a. The surveillance shall be limited in scope and duration to that necessary for the purposes referred to in section A., above.

b. No particular United States person shall be targeted intentionally without consent.

c. The content of any communication shall:

(1) Be retained only when actually needed for the purposes referred to in section A. above,

(2) Be disseminated only to persons conducting the activity,
and

(3) Be destroyed immediately upon completion of the activity.

d. The technical parameters of a communication (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes outlined in section A., above, **or** for collection avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment provided such dissemination and use are limited to the purposes outlined in section A. or collection avoidance purposes. No content of any communication may be retained or used other than as provided in paragraph **B.2.c.**, above.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 6. TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENTA. APPLICABILITY

This part of Procedure 5 applies to the training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment. It does not apply to the interception of communications with the consent of one of the parties to the communication or to the training of intelligence personnel by nonintelligence components.

B. PROCEDURES

1. Training guidance. The training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment shall include guidance concerning the requirements and restrictions of the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and E.O. 12333 (reference (a)), with respect to the unauthorized acquisition and use of the content of communications of United States persons.

2. Training limitations

a. Except as permitted by paragraph B.2.b. and c., below, the use of electronic communications and surveillance equipment for training purposes is permitted, subject to the following limitations:

(1) To the maximum extent practical, use of such equipment for training purposes shall be directed against communications which are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under Parts 1, 2, and 3 of this procedure.

(2) The contents of private communications of nonconsenting United States persons may not be acquired aurally unless the person is an authorized target of electronic surveillance.

(3) The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

b. Public broadcasts, distress signals, or official U.S. Government communications may be monitored, provided that when government agency communications are monitored, the consent of an appropriate official is obtained.

c. Minimal acquisition of information is permitted as required for calibration purposes.

3. Retention and dissemination. Information collected during training that involves communications described in subparagraph B.2.a. (1), above, shall be retained and disseminated in accordance with minimization procedures applicable to that electronic surveillance. Information collected during training that does not involve communications described in subparagraph B.2.a. (1), above, or that is acquired inadvertently, shall be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose. This limitation does not apply to distress signals.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 7: CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYSA. APPLICABILITY AND SCOPE

This part of Procedure 5 applies to the conduct of vulnerability surveys and bearability surveys by DoD intelligence components.

B. EXPLANATION OF UNDEFINED TERMS

1. The term vulnerability survey refers to the acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to **interception** by foreign intelligence services.

2. The term hearability survey refers to monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the quality of reception over time.

C. PROCEDURES

1. Conduct of vulnerability surveys. **Nonconsensual** surveys may be conducted to determine the potential vulnerability to intelligence services of a foreign power of transmission facilities of communications common carriers, other **private** commercial entities, and entities of the federal government, subject of the following limitations:

a. No vulnerability survey may be conducted without the prior written approval of the Director, National Security Agency, or his designee.

b. No transmission may be acquired aurally.

c. No content of any transmission may be acquired by any means.

d. No transmissions may be recorded.

e. No report or **log** may identify any United States person or entity except to the extent of identifying transmission facilities that are vulnerable to surveillance by foreign powers. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, the identity of such users may be obtained but not from the content of the transmissions themselves, and may be included in such report or log. Reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

2. Conduct of bearability surveys. The Director, National Security Agency, may conduct, or may authorize the conduct by other agencies, of hearability surveys of telecommunications that are transmitted in the United States.

a. Collection. When practicable, consent. will be secured from the **owner** or user of the facility against which the bearability survey is to be conducted prior to the commencement of the survey.

b. Processing and Storage. Information collected during a bearability survey must be processed and stored as follows:

(1) The content of communications may not be recorded or included in any report.

(2) No microwave transmission may be demultiplexed or demodulated for any purpose.

(3) No report or log may identify any person or entity except to the extent of identifying the **transmission** facility-that can be intercepted from the intercept site. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the purpose for which the bearability survey has been conducted, the identity of such users may be obtained provided **such identities** may not be obtained from the contents of the transmissions themselves.

c. Dissemination. Reports may be disseminated only within the U.S. Government. Logs may not be disseminated unless required to verify **results** contained in reports.